# *Community Interest and Information Sensitivity*

As a result of the heightened level of interest in the vulnerability of American communities to terrorism following the events of September 11, 2001, the public is likely to be keenly interested in efforts to protect people, buildings, and systems from terrorism and technological disasters. The planning team should understand that this presents both benefits and challenges, because much of the same information that can be used to rally public support for mitigation planning can also be of use to potential terrorists, saboteurs, or others with malevolent intent. For that reason, the planning team must carefully maintain the security of any information that pertains to vulnerabilities, security measures, and response plans. Jurisdictions' legal counsels should be able to provide guidance on how best to protect such sensitive information within the provisions of applicable freedom of information laws.

This constitutes a significant departure from the open and inclusive way in which mitigation planning has historically been conducted. However, new security realities demand that we re-evaluate the way we think about information sensitivity, in particular how, where, when, and with whom we discuss risks, vulnerabilities, and protective (mitigation) measures. In addition to the overarching public safety rationale for protecting this information from those who would use it against us, the planning team should be sensitive to the fact that the owners and operators of many community assets may be reluctant to reveal their own security shortcomings due to concerns about liability, perception of vulnerability or weakness, and general security-consciousness. For communities and states to work effectively with the people, facilities, and systems they are tasked with protecting, working relationships must be based on trust. All project partners should be committed to maintaining the integrity of the planning process as well as the principles and ultimate goal of the process: a more secure built environment.

Thus, managing sensitive information will be a new challenge for many communities and states. The federal government has the option to classify information when appropriate to protect the interest of national security, but most state and local governments currently lack adequate authorities and tools for preventing the inappropriate disclosure of every kind of sensitive data with any certainty. Communities and states should address this problem in two ways: first, they will need to ensure that sensitive information is handled in such a way as to maintain its security, and second, they will need to have adequate protections in place to ensure that sensitive information is not released when it is requested by members of the public who have no justifiable reason (or "need to know") for seeing the information. The following sections elaborate on these two ways to protect sensitive information while maintaining an appropriate level of public involvement in the planning process.

## Internal Handling Procedures

State and local governments may have the ability to assign "For Official Use Only" (FOUO) status or a similar designation to information that is privileged, sensitive, or otherwise should be protected from circulation or disclosure to the public. However, such measures often lack formal information handling procedures and enforceability. Communities are encouraged to review their handling procedures to ensure that sensitive information in their possession can be authoritatively designated as such and protected appropriately, and once proper procedures are in place they should be applied and adhered to rigorously.

## Withholding Sensitive Information

In keeping with the democratic tradition, federal and state laws generally require that government proceedings and documents be accessible to the public. These laws, often called "sunshine laws" or "freedom of information" laws, usually require public access to meetings whenever a commission, committee, board, task force or other official group meets to discuss public business. They also require that most government documents and records be made available to the public upon request.

While these laws seek to keep governmental processes in the open, many of them establish disclosure exemptions for various types of sensitive information. Planners should work with their jurisdiction's legal staff to carefully review the applicable laws and to determine how these laws may impact their ability to protect sensitive planning information. Furthermore, they should also understand the specific procedures required to

withhold documents and hold closed meetings as necessary to protect sensitive information from disclosure to anyone without a "need to know."

## *Suggested Elements and Sample Language for a "For Official Use Only" (FOUO) Policy*

### Definition of FOUO

The term 'For Official Use Only' should apply to information which is sensitive and requires protection from disclosure to the general public, and for which a significant reason, statutory requirement, or regulatory instruction exists to preclude general circulation. FOUO status is not a security classification level.

### Guidelines for Determining Sensitivity

Information that may qualify for FOUO status includes the design, construction, security, and protection of government facilities and critical infrastructures; assessments of the vulnerabilities of facilities and systems; plans, procedures, and protocols for responding to terrorist attacks or other criminal events; or any other information that could be used for the purposes of damaging or destroying any facility or disrupting any operations.

### Designation of Authority

Authority to assign and remove FOUO status should be granted to designated personnel based on position and/ or responsibilities.

### Document Marking Requirements

Information that has been designated FOUO should be plainly marked as such for ease of recognition. To promote proper protection of information, markings should be applied at the time documents are drafted or as soon as FOUO information is added. Materials containing FOUO information should be marked

PROPERTY OF (JURISDICTION NAME)
FOR OFFICIAL USE ONLY

at the bottom of the front cover, title page, first page and outside of the back cover. Additionally, each page containing FOUO information should be similarly marked at the bottom. Material other than paper documents such as slides, computer media, films, etc., should also bear these markings. Electronically transmitted messages (e.g., e-mails) containing FOUO information should have the abbreviation 'FOUO' before the beginning of the text.

### Handling Instructions

FOUO material should never be left unattended, and reasonable steps should be taken to minimize the risk of access by anyone without a "need to know." After working hours, FOUO information should be stored in a locked desk, file cabinet, bookcase, or similar location. Restrictions may also be placed on the duplication and transmission of FOUO information.